COMPUTER INCIDENT REPORTING FORM

Use this form to report security incidents to the Chief Information Officer of the Commonwealth. If additional information is required, you will be contacted via phone or email. To assist with our initial assessment and investigation, please provide as much information as possible. Fax completed form to 804-371-5235.

STATUS

□ Site Under Attack □ Past Incident □ Repeated Incidents, unresolved

CONTACT INFORMATION

Name/Last______________________________First___________________________MI_____Title_________________________________

Organization____

E-mail____

Phone _(_____)____________________________________ FAX _(_____)____

Location/Site(s) Involved____

Street Address Involved____

City____State__________________ZIP____

INCIDENT DESCRIPTION

□ Denial of Service □ Unauthorized access (e.g. Intrusion/Hack)

□ Website Defacement

□ Malicious Code (e.g. virus/worm or trojan)

□ Threat/harassment via electronic medium (includes employees)

□ Misuse of Systems (internal or external, includes inappropriate use by employees)

□ Other (specify)____

DATE/TIME OF INCIDENT DISCOVERY

Date____Time____

Duration of Incident____

How did you detect this?____

Has the incident been resolved? Explain____

WHO ELSE HAS BEEN NOTIFIED (CHECK ALL THAT APPLY)?

□ System administrator □ Department Director/Data Owner □ Human Resources

□ General Counsel □ Law Enforcement (who & when) ____

□ Other (Please Specify) ____

IMPACT OF INCIDENT

□ Loss/Compromise of Data □ System Downtime

□ Damage to Systems □ Other Organizations' Systems Affected

□ Financial Loss (estimated amount: $________________________)

□ Damage to the Integrity or Delivery of Critical Goods, Services or Information

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

□ High (defaced websites) □ Medium (Trojan detected) □ Low (Small virus outbreak)

□ Unknown

SENSITIVITY OF DATA

□ High (Privacy Act violation) □ Medium (local administration) □ Low (Public materials)

□ Unknown

IDENTIFY THE COMPUTER OPERATING SYSTEM AND ANY OTHER SOFTWARE INVOLVED (CHECK ALL THAT APPLY)

□ Unix □ OS2 □ Linux □ VAX/VMS

□ Microsoft _ XP _2000 _NT _95/98 □ Novell □ Sun OS/Solaris

□ Other Software (Specify) ____

WHAT STEPS HAVE YOU TAKEN TO RESPOND (CHECK ALL THAT APPLY)?

□ No action taken □ System disconnected from network

□ Restored data from backup □ Updated virus definitions & scanned hard drive

□ Log files examined (saved and secured) □ Physically secured computer

□ Other (specify) ____